PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 14 September 1999 (14.09.99)	
International application No. PCT/RU98/00182	**Applicant's or agent's file reference** 155A
International filing date (day/month/year) 19 June 1998 (19.06.98)	**Priority date** (day/month/year) 19 January 1998 (19.01.98)
Applicant MOLDOVYAN, Alexandr Andreevich et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

30 July 1999 (30.07.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Beatriz Morariu

Telephone No.: (41-22) 338.83.38

PCT

ВСЕМИРНАЯ ОРГАНИЗАЦИЯ
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
Международное бюро

ВОИС

МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С ДОГОВОРОМ О ПАТЕНТНОЙ КООПЕРАЦИИ (PCT)

(51) Международная классификация изобретения [6]: H01L 9/00	A1	(11) Номер международной публикации: **WO 99/36942** (43) Дата международной публикации: 22 июля 1999 (22.07.99)

(21) Номер международной заявки: PCT/RU98/00182

(22) Дата международной подачи: 19 июня 1998 (19.06.98)

(30) Данные о приоритете:
98100685 19 января 1998 (19.01.98) RU

(71) Заявитель *(для всех указанных государств, кроме US)*: ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "МОСКОВСКАЯ ГОРОДСКАЯ ТЕЛЕФОННАЯ СЕТЬ" [RU/RU]; 103804 Москва, ГСП, Дегтярный переулок, д. 6, строение 2 (RU) [OTKRYTOE AKTSIONERNOE OBSCHESTVO "MOSKOVSKAYA GORODSKAYA TELEPHONNAYA SET", Moscow (RU)]

(71)(72) Заявители и изобретатели: МОЛДОВЯН Александр Андреевич [RU/RU]; 188710 Всеволожск, ул. Александровская, д. 88/2, кв. 62 (RU) [MOLDOVYAN, Alexandr Andreevich, Vsevolozhsk (RU)]. МОЛДОВЯН Николай Андреевич [RU/RU]; 188710 Всеволожск, ул. Александровская, д. 88/2, кв. 58 (RU) [MOLDOVYAN, Nikolai Andreevich, Vsevolozhsk (RU)].

(74) Агент: ООО ЦЕНТР ИННОТЕК; 105023 Москва, ул. Б. Семёновская, 49-404 (RU) [OOO TSENTR INNOTEK, Moscow (RU)].

(81) Указанные государства: CN, CZ, JP, KR, PL, SI, SK, UA, US, европейский патент (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

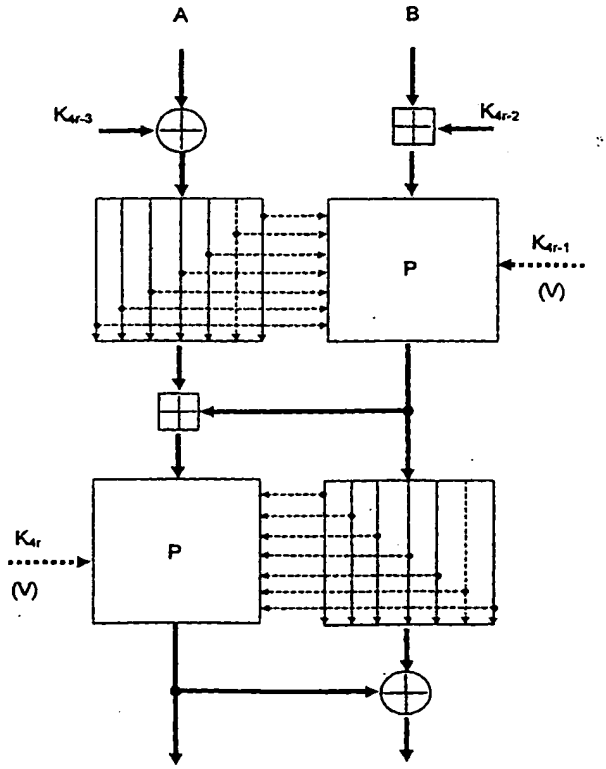
Опубликована
С отчётом о международном поиске.

(54) Title: METHOD FOR THE CRYPTOGRAPHIC CONVERSION OF BINARY DATA BLOCKS

(54) Название изобретения: СПОСОБ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ БЛОКОВ ДВОИЧНЫХ ДАННЫХ

(57) Abstract

The present invention pertains to the field of electrical communications and computer techniques and more precisely relates to cryptographic methods and devices for the ciphering of digital data. This method comprises splitting a data block into $N \geq 2$ sub–blocks and sequentially converting said sub–blocks by applying at least one conversion operation on the i–th sub–block, where $i \leq N$, said operation depending on the value of the j–th sub–block where $j \leq N$. This method is characterised in that the operation depending on the value of the j–th sub–block is a transposition operation of the bits in the i–th sub–block. This method is also characterised in that the transposition operation of the bits in the i–th sub–block, which depends on the value of the j–th sub–block, is carried out according to a secret key before the beginning of the i–th sub–block conversion. This method is further characterised in that a binary vector V is determined prior to the current transposition operation of the bits in the i–th sub–block, which depends on the j–th sub–block, wherein said transposition operation of the bits in the i–th sub–block is carried out according to the value of the vector V. The binary vector is determined according to its value when carrying out the preceding conversion step of one of the sub–blocks and according to the value of the j–th sub–block.



(57) Реферат

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования цифровых данных. Способ заключается в разбиении блока данных на $N \geqslant 2$ подблоков, поочередном преобразовании подблоков путем выполнения над i-тым, где $i < N$, подблоком по крайней мере одной операции преобразования, которая зависит от значения j-того, где $j < N$, подблока. Новым в заявляемом способе является то, что в качестве операции, зависящей от значения j-того подблока, используется операция перестановки битов i-того подблока. Новым является также то, что операция перестановки битов i-того подблока, зависящая от значения j-того подблока, формируется в зависимости от секретного ключа до начала преобразования i-того подблока. Кроме того новым является то, что перед осуществлением текущей операции перестановки битов i-того подблока, зависящей от j-того подблока, дополнительно формируют двоичный вектор V, а операцию перестановки битов i-того подблока осуществляют в зависимости от значения V, причем двоичный вектор формируют в зависимости от его значения в момент выполнения предшествующего шага преобразования одного из подблоков и от значения j-того подблока.

Способ криптографического преобразования блоков двоичных данных

Область техники

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации).

Предшествующий уровень техники

В совокупности признаков заявляемого способа используются следующие термины:

-секретный ключ представляет из себя двоичную информацию, известную только законному пользователю;

-криптографическое преобразование - это преобразование цифровой информации, которое обеспечивает влияние одного бита исходных данных на многие биты выходных данных, например, с целью защиты информации от несанкционированного чтения, формирования цифровой подписи, выработки кода обнаружения модификаций; одними из важных видов криптографических преобразований являются одностороннее преобразование, хэширование и шифрование;

-хэширование информации есть некоторый способ формирования так называемого хэш-кода, размер которого является фиксированным (обычно 128 бит) для сообщений любого размера; широко применяются способы хэширования, основанные на итеративных хэш-функциях с использованием блочных механизмов криптографического преобразования информации [см. Lai X., Massey J.L. Hash Functions Based on Block Ciphers/Workshop on the Theory and Applications of Cryptographic Techniques. EUROCRYPT'92. Hungary, May 24-28, 1992. Proceedings. P. 53-66.].

-шифрование есть процесс, преобразования информации, который зависит от секретного ключа и преобразует исходный текст в шифртекст, представляющий собой псевдослучайную последовательность знаков, из которой получение информации без знания секретного ключа практически неосуществимо;

-дешифрование есть процесс, обратный процедуре шифрования; дешифрование обеспечивает восстановление информации по криптограмме при знании секретного ключа;

-шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием секретного ключа; шифр может быть реализован в виде программы для ЭВМ или в виде отдельного устройства;

-двоичный вектор - это некоторая последовательность нулевых и единичных битов, например 101101011; конкретная структура двоичного вектора может быть интерпретирована как двоичное число, если считать, что позиция каждого бита соответствует двоичному разряду, т.е. двоичному вектору может быть сопоставлено численное значение, которое определяется однозначно структурой двоичного вектора;

-криптоанализ - метод вычисления секретного ключа для получения несанкционированного доступа к зашифрованной информации или разработка метода, обеспечивающего доступ к зашифрованной информации без вычисления секретного ключа;

-одностороннее преобразование - это такое преобразование L-битового входного блока данных в L-битовый выходной блок данных, которое позволяет легко вычислить выходной блок по входному блоку, а вычисление входного блока, который бы преобразовывался в случайно выбранный выходной блок, является практически невыполнимой задачей;

-односторонняя функция - это функция, значение которой легко вычисляется по данному аргументу, однако вычисление аргумента по данному значению функции является вычислительно трудной задачей; односторонние функции реализуются как последовательность процедур одностороннего преобразования некоторого входного блока (аргумента), выходное значение которого принимается за значение функции;

-криптостойкость является мерой надежности защиты зашифрованной информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации

по криптограмме при знании алгоритма преобразования, но без знания секретного ключа; в случае односторонних преобразований под криптостойкостью понимается сложность вычисления входного значения блока по его выходному значению;

-операции циклического сдвига, зависящие от преобразуемых подблоков или зависящие от двоичного вектора - это операции циклического сдвига на число бит, задаваемое значением подблока или значением двоичного вектора; операции циклического сдвига влево (вправо) обозначаются знаком "<<<"(">>>"), например, запись $B_1<<<B_2$ обозначает операцию циклического сдвига влево подблока B_1 на число бит равное значению двоичного вектора B_2; подобные операции являются базовыми для шифра RC5;

-одноместная операция - это операция выполняемая над одним операндом (блоком данных или двоичным вектором); значение подблока после выполнения некоторой данной одноместной операции зависит только от его начального значения; примером одноместных операций являются операции циклического сдвига;

-двухместная операция - это операция выполняемая над двумя операндами; результат выполнения некоторой данной двухместной операции зависит от значения каждого операнда; примером двухместных операций являются операции сложения, вычитания, умножения и др.

Известны способы блочного шифрования данных, см. например стандарт США DES [National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, January 1977]. В данном способе шифрование блоков данных выполняют путем формирования секретного ключа, разбиения преобразуемого блока данных на два подблока L и R и поочередного изменения последних путем выполнения операции поразрядного суммирования по модулю два над подблоком L и двоичным вектором, который формируется как выходное значение некоторой функции F от значения подблока R. После этого блоки переставляются местами.

Функция F в указанном способе реализуется путем выполнения операций перестановки и подстановки, выполняемых над подблоком R. Данный способ обладает высокой скоростью преобразований при реализации в виде специализированных электронных схем.

Однако, известный способ-аналог использует секретный ключ малого размера (56 бит), что делает его уязвимым к криптоанализу на основе подбора ключа. Последнее связано с высокой вычислительной мощностью современных ЭВМ массового применения.

Наиболее близким по своей технической сущности к заявляемому способу криптографического преобразования блоков двоичных данных является способ, реализованный в шифре RC5 описанный в работе [R.Rivest, The RC5 Encryption Algorithm/ Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994),Lecture Notes in Computer Science, v. 1008, Springer-Verlag, 1995, pp.86-96]. Способ прототип включает в себя формирование секретного ключа в виде совокупности подключей, разбиение входного блока данных на подблоки A и B, и поочередное преобразование подблоков. Подблоки преобразуются путем выполнения над ними одноместных и двухместных операций. В качестве двухместных операций используются операции сложения по модулю 2^n, где n=8,16,32,64, и операция поразрядного суммирования по модулю 2. В качестве одноместной операции используется операция циклического сдвига влево, причем число бит на которое сдвигается преобразуемый подблок зависит от значения другого подблока, это определяет зависимость операции циклического сдвига на текущем шаге преобразования подблока от исходного значения входного блока данных. Двухместная операция выполняется над подблоком и подключом, а также над двумя подблоками. Характерным для способа прототипа является использование операции циклического сдвига битов одного из подблоков, зависящей от значения другого подблока.

Подблок, например подблок B, преобразуют следующим путем. Выполняется операция поразрядного суммирования по модулю 2 ("⊕") над подблоками A и B и значение, получаемое после выполнения этой операции, присваивается подблоку B. Это записывается в виде соотношения:

$$B \leftarrow B \oplus A,$$

где знак "←" обозначает операцию присваивания. После этого над подблоком B выполняют операцию циклического сдвига на число бит равное значению подблока A:

$$B \leftarrow B \lll A.$$

Затем над подблоком и одним из подключей S выполняют операцию суммирования по модулю 2^n: $B \leftarrow (B + S) \bmod 2^n$, где n - длина подблока в битах. После этого аналогичным образом преобразуется подблок A. Выполняется несколько таких шагов преобразования обоих подблоков.

Данный способ обеспечивает высокую скорость шифрования при реализации в виде программы для ЭВМ или в виде электронных устройств шифрования. Однако, способ прототип имеет недостатки, а именно, он не обеспечивает высокой стойкости криптографического преобразования данных к дифференциальному и линейному криптоанализу [Kaliski B.S., Yin Y.L. On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm. Advances in Cryptology-CRYPTO'95 Proceedings, Springer-Verlag, 1995, pp. 171-184]. Этот недостаток связан с тем, что эффективность использования операций, зависящих от преобразуемых данных, с целью повышения стойкости шифрования к известным методам криптоанализа снижается тем, что число потенциально реализуемых вариантов операции циклического сдвига равно числу двоичных разрядов подблока n и не превышает 64.

В основу изобретения положена задача разработать способ криптографического преобразования блоков двоичных данных, в котором преобразование входных данных осуществлялось бы таким образом, чтобы обеспечивалось повышение числа различных вариантов операции, зависящей от преобра-

зуемого блока, благодаря чему повышается стойкость к дифференциальному и линейному криптоанализу.

Раскрытие изобретения

Поставленная задача достигается тем, что в способе криптографического преобразования блоков двоичных данных, заключающемся в разбиении блока данных на $N \geqslant 2$ подблоков, поочередном преобразовании подблоков путем выполнения над i-тым, где $i < N$, подблоком по крайней мере одной операции преобразования, зависящей от значения j-ого, где $j < N$, подблока, новым, согласно изобретению, является то, что в качестве операции, зависящей от значения j-того подблока используется операция перестановки битов i-того подблока.

Благодаря такому решению увеличивается число возможных вариантов операции, зависящей от значения j-того подблока, что обеспечивает повышение стойкости криптографического преобразования к дифференциальному и линейному криптоанализу.

Новым является также то, что операция перестановки битов i-того подблока, зависящая от значения j-ого подблока, формируется в зависимости от секретногоключа до начала преобразования i-того подблока.

Благодаря такому решению, модификация операции перестановки битов i-того подблока, зависящая от значения j-того подблока, не является заранее предопределенной, что обеспечивает дополнительное повышение стойкости криптографического преобразования к дифференциальному и линейному криптоанализам и позволяет уменьшить число операций преобразования и тем самым увеличить скорость шифрования.

Новым является также то, что перед осуществлением текущей операции перестановки битов i-того подблока, зависящей от j-того подблока, дополнительно формируют двоичный вектор V, а операцию перестановки битов i- подблока осуществляют в зависимости от значения V, причем двоичный вектор формируют в зависимости от его значения в момент выполнения предшествующего шага преобразования одного из подблоков и от значения j-ого подблока.

Благодаря такому решению, обеспечивается дополнительное повышение криптостойкости к атакам, основанным на сбоях устройства шифрования.

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи.

Краткое описание чертежей

На фиг. 1 представлена обобщенная схема криптографического преобразования согласно заявляемому способу.

На фиг. 2 схематично представлена структура блока управляемых перестановок.

На фиг. 3 представлена структура блока управляемых перестановок с 32-битовым информационным входом.

На фиг. 4 представлена блок-схема элементарного переключателя.

На фиг. 5 представлена таблица входных и выходных сигналов элементарного переключателя при управляющем сигнале u=1.

На фиг. 6 представлена таблица входных и выходных сигналов элементарного управляемого переключателя при значении управляющего сигнала u=0.

Лучшие варианты осуществления изобретения

Изобретение поясняется обобщенной схемой криптографического преобразования блоков данных на основе заявляемого способа, которая представлена фиг. 1,

где: P - блок управляемых перестановок; A и B - преобразуемые n-битовые подблоки; K_{4r}, K_{4r-1}, K_{4r-2}, K_{4r-3} - n-битовые элементы секретного ключа (n-битовые подключи); V - двоичный вектор, формируемый в зависимости от входных данных; знак $\oplus$ обозначает операцию поразрядного суммирования по модулю два; знак $\boxplus$ - операцию суммирования по модулю n, где n - длина подблока данных в битах. Жирные сплошные линии обозначают шину передачи n-битовых сигналов, тонкие сплошные линии - передачу одного бита, тонкие пунктирные линии - передачу одного управляющего бита. Жирные пунктирные линии - шину передачи n управляющих сигналов, в

качестве которых используются биты подключей или биты двоичного вектора. Использование битов подключа в качестве управляющих сигналов обеспечивает формирование конкретной модификации операции перестановки битов подблока, зависящей от значения входного блока, что дополнительно повышает стойкость криптографического преобразования.

Фиг. 1 показывает один раунд преобразований. В зависимости от конкретной реализации блока управляемых перестановок и требуемой скорости преобразований могут быть заданы от 2 до 16 и более раундов. Данная схема процедур криптографических преобразований может использоваться для осуществления шифрования и для осуществления односторонних преобразований. В последнем случае секретный ключ не используется и вместо сигналов подключей на управляющий вход блока P подаются сигналы двоичного вектора V, формируемого в зависимости от значения преобразуемых подблоков на промежуточных шагах преобразования. При выполнении шифрования одни и те же четыре n-битовых подключа K_4, K_3, K_2 и K_1 могут использоваться при выполнении каждого раунда шифрования. В этом случае при типичном размере подблока n=32 длина секретного ключа составляет 128 бит. При использовании секретного ключа большего размера в каждом раунде могут использоваться четыре независимых подключа K_{4r}, K_{4r-1}, K_{4r-2} и K_{4r-3}. Например, при числе раундов r=3 в первом раунде используются подключи K_4, K_3, K_2 и K_1, во втором раунде - подключи K_8, K_7, K_6 и K_5, в третьем раунде - подключи K_{12}, K_{11}, K_{10} и K_9.

Возможность технической реализации заявляемого способа поясняется следующими конкретными примерами его осуществления.

Пример 1.

Данный пример относится к использованию способа для шифрования данных. Секретный ключ представлен в виде четырех подключей K_{4r}, K_{4r-1}, K_{4r-2} и K_{4r-3}. Один раунд шифрования описывается следующей последовательностью процедур:

1. Преобразовать подблок A в соответствии с выражением:

$$A \leftarrow A \oplus K_{4r-3},$$

где "←" - обозначение операции присваивания.

2. Преобразовать подблок B в соответствии с выражением:

$$B \leftarrow B \boxplus K_{4r-2}.$$

3. В зависимости от значения подблока A и от подключа K_{4r-1} осуществить перестановку битов подблока B.

4. Преобразовать подблок A в соответствии с выражением:

$$A \leftarrow A \boxplus B.$$

5. В зависимости от значения подблока B и от подключа K_{4r} осуществить перестановку битов подблока A.

6. Преобразовать подблок B в соответствии с выражением:

$$B \leftarrow B \oplus A.$$

Пример 2.

Данный пример описывает один раунд односторонних преобразований, в соответствии со следующей последовательностью процедур:

1. Сформировать двоичный вектор V:

$$V \leftarrow A \lll B.$$

2. Преобразовать подблок B в соответствии с выражением:

$$B \leftarrow B \boxplus V.$$

3. Сформировать двоичный вектор V в зависимости от его значения на предыдущем шаге и от значения подблоков A и B в соответствии с формулой:

$$V \leftarrow (V \lll A) \oplus (B \lll 13).$$

4. Преобразовать подблок A в соответствии с выражением:

$$A \leftarrow A \oplus V.$$

5. В зависимости от значений A и V осуществить перестановку битов подблока B.

6. Преобразовать подблок A в соответствии с выражением:

$$A \leftarrow A \boxplus B.$$

7. Сформировать двоичный вектор V:

$$V \leftarrow (V <<< B) \oplus (A <<< 11).$$

8. В зависимости от значений B и V осуществить перестановку битов подблока A.

9. Преобразовать подблок B в соответствии с выражением:

$$B \leftarrow B \oplus A.$$

На фиг. 2 показана возможная реализация блока управляемых перестановок, использующая совокупность элементарных переключателей S. Данный пример соответствует блоку P с 8-битовым входом для сигналов данных и 8-битовым входом для управляющих сигналов, обозначенных пунктирными линиями аналогично обозначению на фиг. 1.

Число различных вариантов операции перестановки равно числу возможных кодовых комбинаций на входе управления и составляет для блока P со структурой, представленной на фиг. 2, $2^8=256$, что превышает число операций циклического сдвига, используемых в способе прототипе. Аналогичным способом может быть составлена схема для блока P с произвольными размерами входа для данных и входа для управляющих сигналов, в частности для блока P с 32-битовым входом данных и 32-битовым входом для управляющих сигналов. В последнем случае достигается число различных вариантов операции перестановки равное $2^{32} > 10^9$.

Фиг. 3 показывает структуру блока управляемых перестановок с 32-битовым входом для данных и 79-битовым управляющим входом. Данный блок управляемых перестановок реализует уникальную перестановку входных двоичных разрядов для каждого возможного значения кодовой комбинации на управляющем входе, число которых составляет 2^{79}. Внешние информационные входы блока управляемых перестановок обозначены i1, i2,..., i32, внешние выходы обозначены o1, o2,...,o32

управляющие входы обозначены c1, c2, ..., c79. Элементарные переключатели S соединены таким образом, что они образуют матрицу состоящую из 31 строки. В первой строке соединены 31 элементарных переключателей S, во второй строке - 30, в третьей - 29 и т.д. В каждой последующей строке число элементарных переключателей уменьшается на 1. В самой нижней 31-й строке соединен 1 элементарный переключатель.

Строка с номером $j \neq 31$ имеет 33-j входов, 33-j выходов и 32-j управляющих входа. Последний (самый правый) выход j-ой строки является внешним выходом блока управляемых перестановок, оставшиеся 32-j выхода j-строки соединены с соответствующими входами (j+1)-й строки. Последняя 31-я строка имеет два выхода и оба из них являются внешними выходами блока управляемых перестановок. Не более, чем на один управляющий вход каждой строки подается единичный (u=1) управляющий сигнал. Для обеспечения этого требования служат двоично-тридцатидвухричные дешифраторы $F_1, F_2, \ldots, F_{15}$ и двоично-шестнадцатиричный дешифратор F_{16}. Дешифраторы $F_1, F_2, \ldots, F_{15}$ имеют пять внешних управляющих входов, на которые подается произвольный 5-битовый двоичный код, и 32 выхода. Дешифраторы вырабатывают только на одном выходе единичный сигнал. На оставшихся 31 выходе устанавливается нулевой сигнал. Дешифратор F_{16} имеет 4 входа, на которые подается произвольный 4-битовый двоичный код, и 16 выходов, из которых только на одном устанавливается единичный сигнал. Для всех дешифраторов $F_1, F_2, \ldots, F_{15}$ и F_{16} каждое входное значение двоичного кода задает единственно возможный номер выхода, на котором устанавливается единичный сигнал (u=1).

Часть выходов дешифратора F_h, где $h \leq 15$, соединены с управляющими входами h-ой строки (32-h выходов), а часть выходов - с управляющими входами (32-h)-ой строки (оставшиеся h выходов дешифратора). В каждой строке не более, чем на одном элементарном переключателе устанавливается управляющий сигнал u=1. Вход строки, присоединенный к правому входу элементарного переключателя, на который по-

дан единичный управляющий сигнал, коммутируется с внешним выходом блока управляемых перестановок, соответствующим данной строке. Если единичный управляющий сигнал подан на самый левый элементарный переключатель, то с внешним выходом блока управляемых перестановок (блок Р) коммутируется самый левый вход строки. Первая строка коммутирует один из внешних входов i1, i2, . . . , i32 блока Р с внешним выходом o1, а остальные 31 внешних входа - с входами второй строки. Вторая стока коммутирует один из оставшихся 31 внешнего входа с внешним выходом o2, а оставшиеся 30 внешних входов - с входами 3-ей строки и т.д. Такая структура блока Р реализует уникальную перестановку входных битов для каждого значения двоичного кода поданного на 79-битовый управляющий вход блока Р.

Возможен, например, следующий вариант использования управляющего 79-битового входа в схеме криптографического преобразования, показанной на фиг. 1. В качестве управляющих сигналов используются 32 бита, например, подблока В и 47 битов секретного ключа. В качестве последних, например, могут использоваться 32 бита подключа K_{4r-1} и 15 битов подключа K_{4r-2}. В этом случае при введении секретного ключа в устройство шифрования в зависимости от этих 47 битов секретного ключа формируется одна из 2^{47} различных модификаций операции перестановки битов, зависящей от значения входного блока. При этом каждая модификация этой операции включает 2^{32} различных операций перестановки битов подблока А, выбор которых определяется значением подблока В. Выбор модификации не является заранее предопределенным, поскольку он определяется секретным ключом. Это дополнительно повышает стойкость криптографического преобразования. Если в устройстве шифрования используются 4 блока Р, имеющих структуру, показанную на фиг. 3, то число возможных комбинаций модификаций операций перестановок, устанавливаемых на блоках Р в зависимости от секретного ключа, может быть задано до $(2^{47})^4=2^{188}$ при использовании секретного ключа

длиной не менее 188 бит.

Фиг. 4 поясняет работу элементарного переключателя, где u - управляющий сигнал, a и b - входные сигналы данных, c и d - выходные сигналы данных.

Таблицы на фиг. 5 и 6 показывают зависимость выходных сигналов от входных и управляющих сигналов. Из данных таблиц видно, что при u=1 линия a коммутируется с линией c, а линия b - с линией d. При u=0 линия a коммутируется с линией d, а линия b - с линией d.

Благодаря простой структуре современная планарная технология изготовления интегральных схем позволяет легко изготовить криптографические микропроцессоры, содержащие управляемые блоки перестановок с размером входа 32 и 64 бит.

Приведенные примеры показывают, что предлагаемый способ криптографических преобразований блоков двоичных данных технически реализуем и позволяет решить поставленную задачу.

Промышленная применимость

Заявляемый способ может быть реализован, например, в специализированных криптографических микропроцессорах, обеспечивающих скорость шифрования порядка 1 Гбит/с, достаточную для шифрования в масштабе реального времени данных, передаваемых по скоростным оптоволоконным каналам связи.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ криптографического преобразования блоков двоичных данных, заключающийся в разбиении блока данных на $N \geq 2$ подблоков, поочередном преобразовании подблоков путем выполнения над i-тым, где $i \leq N$, подблоком по крайней мере одной операции преобразования, зависящей от значения j-того подблока, о т л и ч а ю щ и й с я тем, что в качестве операции, зависящей от значения j-того, где $j \leq N$, подблока используется операция перестановки битов i-того подблока.

2. Способ по п.1, о т л и ч а ю щ и й с я тем, что операция перестановки битов i-того подблока, зависящая от значения j-того подблока, формируется в зависимости от секретного ключа до начала преобразования i-того подблока.

3. Способ по п.1, о т л и ч а ю щ и й с я тем, что перед осуществлением текущей операции перестановки битов i-того подблока, зависящей от значения j-того подблока, дополнительно формируют двоичный вектор V, а операцию перестановки битов i-того подблока осуществляют в зависимости от значения V, причем двоичный вектор формируют в зависимости от его значения в момент выполнения предшествующего шага преобразования одного из подблоков и от значения j-того подблока.

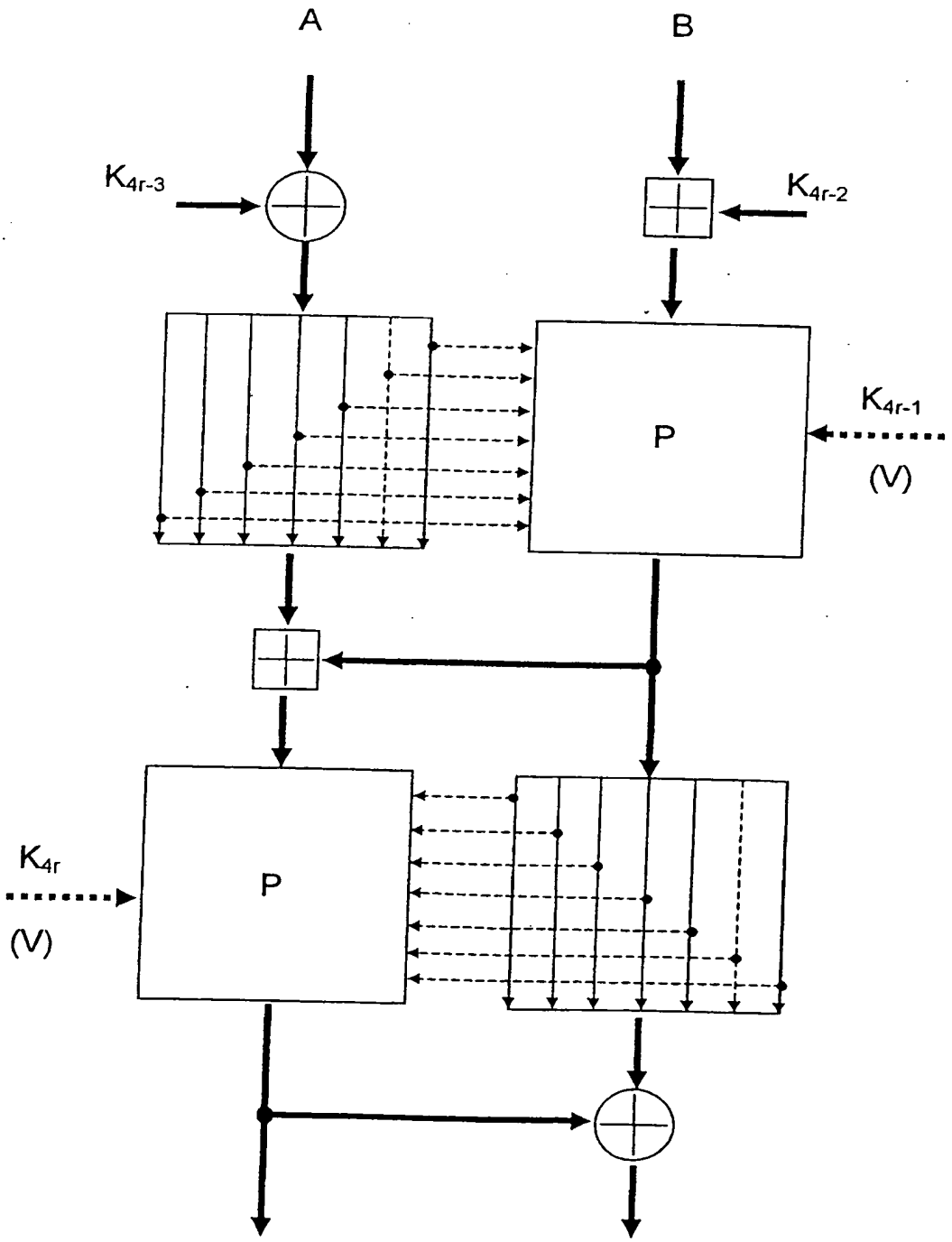


Fig.1.

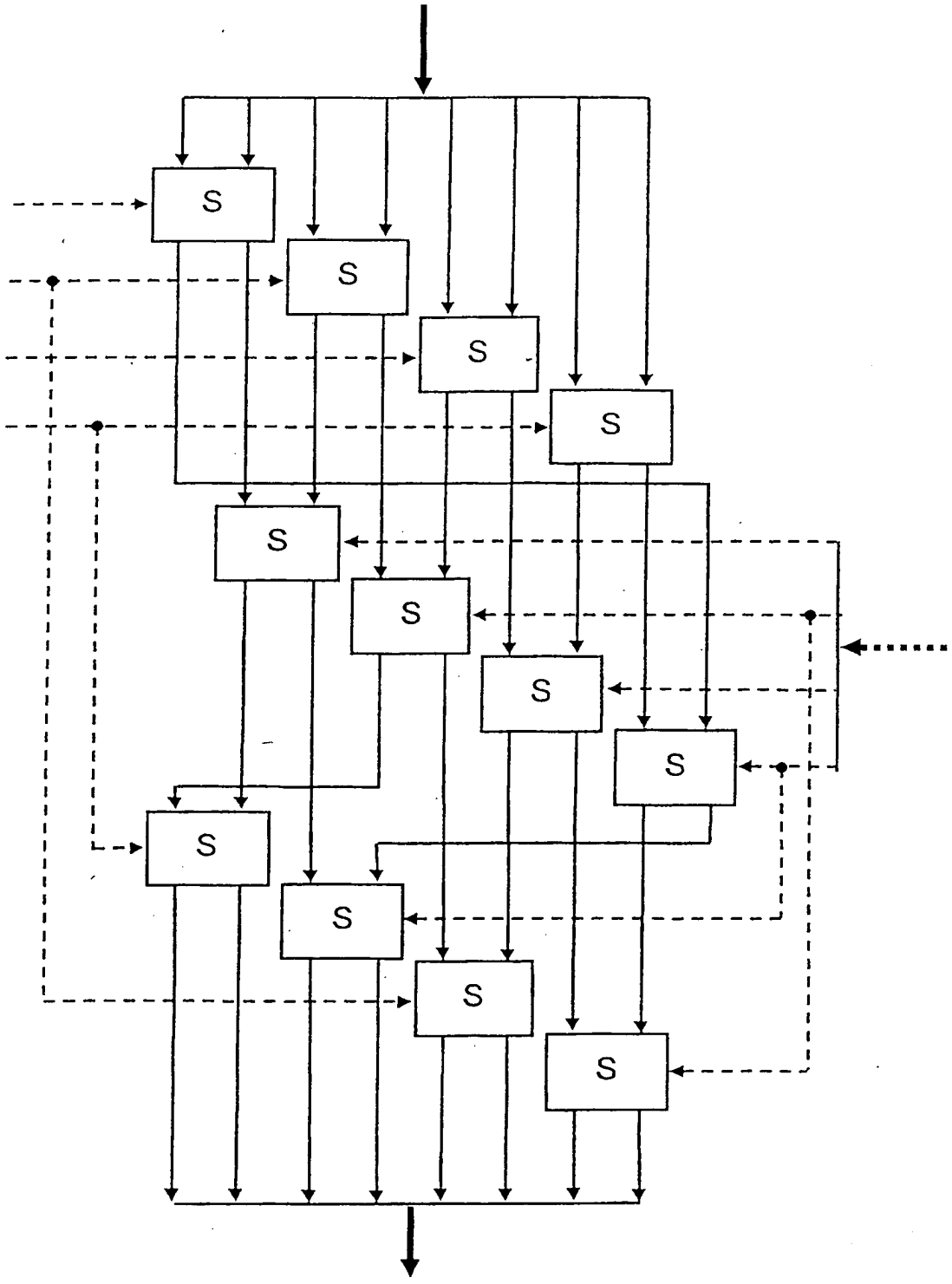


Fig.2.

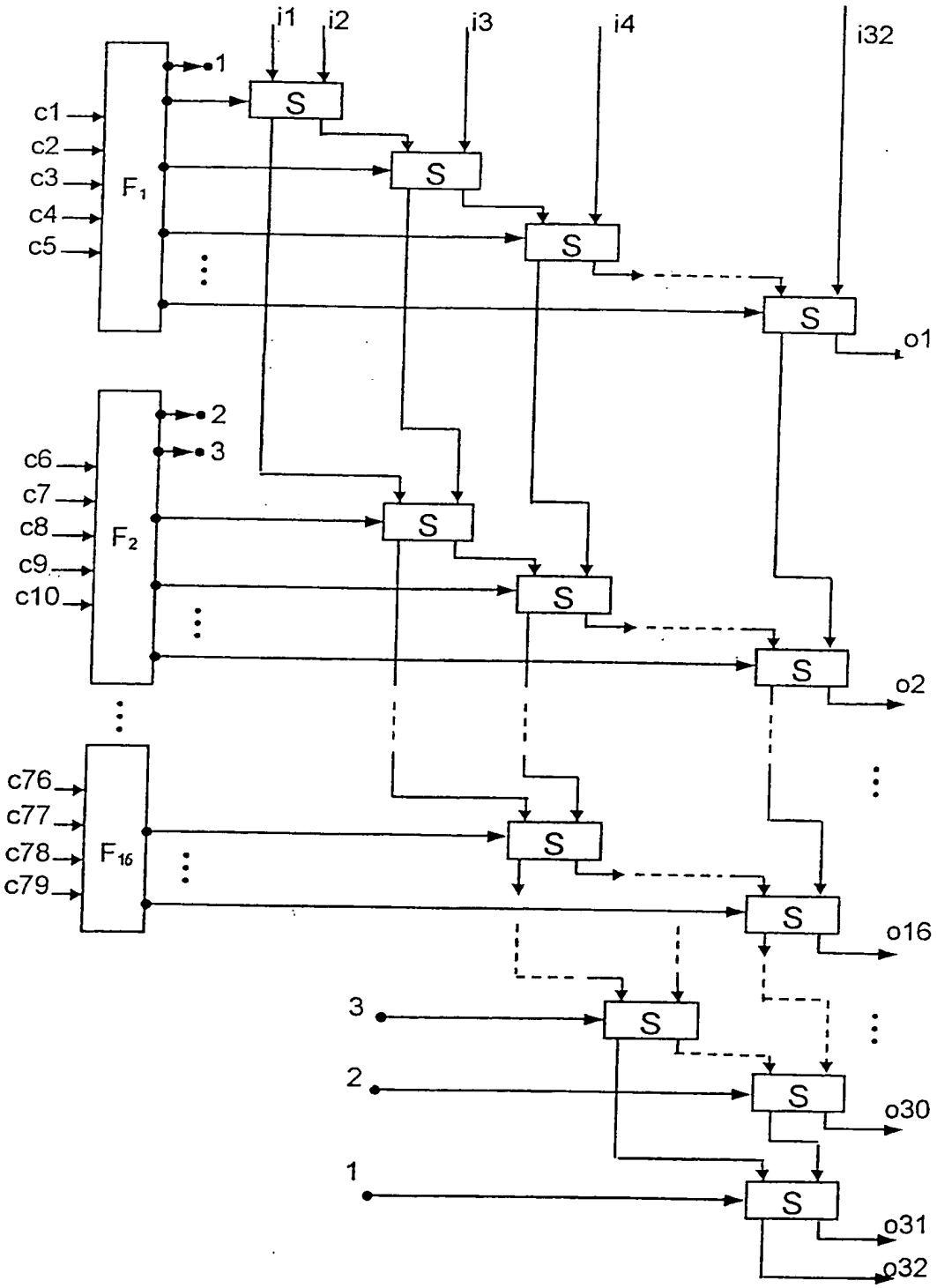

i1
i2
i3
i4
i32
c1
c2
c3
c4
c5
F1
1
S
o1
c6
c7
c8
c9
c10
F2
2
3
o2
c76
c77
c78
c79
F16
o16
3
2
1
o30
o31
o32

Fig. 3.

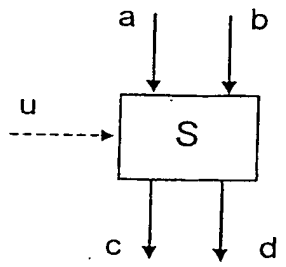


Fig.4.

u=1

INPUT		OUTPUT	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

Fig.5.

u=0

INPUT		OUTPUT	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

Fig.6.

ОТЧЕТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Международная заявка № PCT/RU 98/00182

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:
H01L 9/00
Согласно международной патентной классификации (МПК-6)

B. ОБЛАСТИ ПОИСКА:

Проверенный минимум документации (система классификации и индексы) МПК-6:
H01L 9/00, H04L 9/08, H04L 9/14, H04L 9/28, H04K 1/00

Другая проверенная документация в той мере, в какой она включена в поисковые подборки:

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, поисковые термины):

C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	RU 2097931 C1 (БЕРЕЗИН БОРИС ВЛАДИМИРОВИЧ и др.) 21.11.97	1 - 3
A	EP 0676876 A1 (INTERNATIONAL BUSINESS MASHINES CORPORATION) 11.10.95	1 - 3
A	US 5001754 A (THE TRUSTEED OF PRINCETON UNIVERSITY) Mar. 19, 1991	1 - 3
A	US 5548648 A (INTERNATIONAL BUSINESS MACHINES Corp.) Aug. 20, 1996	1 - 3
A	WO 88/01119 A1 (BRITISH BROADCASTING Corp.) 11 February 1988 (11.02.88)	1 - 3
A	EP 0202989 A1 (THOMSON-CSF) 26.11.86	1 - 3

☐ последующие документы указаны в продолжении графы C.
☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:
"A" документ, определяющий общий уровень техники
"E" более ранний документ, но опубликованный на дату международной подачи или после нее
"O" документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета
"T" более поздний документ, опубликованный после даты приоритета и приведенный для понимания иззобретения
"X" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень
"Y" документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории
"&" документ, являющийся патентом-аналогом

Дата действительного завершения международного поиска
15 сентября 1998 (15.09.98)

Дата отправки настоящего отчета о международном поиске 14 октября 1998 (14.10.98)

Наименование и адрес Международного поискового органа:
Федеральный институт
промышленной собственности
Россия, 121858, Москва, Бережковская наб., 30-1
Факс: 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо:
Д.Смирнов
Телефон №: (095)240-5888

Форма PCT/ISA/210 (второй лист) (июль 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 98/00182

A. CLASSIFICATION OF SUBJECT MATTER [6]:

H01L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H01L 9/00, H04L 9/08, H04L 9/14, H04L 9/28, H04K 1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RU 2097931 C1 (BEREZIN BORIS VLADIMIROVICH et al) 21 November 1997 (21.11.97)	1 - 3
A	EP 0676876 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 11 October 1995 (11.10.95)	1 - 3
A	US 5001754 A (THE TRUSTEED OF PRINCETON UNIVERSITY) 19 March 1991 (19.03.91)	1 - 3
A	US 5548648 A (INTERNATIONAL BUSINESS MACHINES Corp.) 20 August 1996 (19.08.96)	1 - 3
A	WO 88/01119 A1 (BRITISH BROADCASTING Corp.) 11 February 1988 (11.02.88)	1 - 3
A	EP 0202989 A1 (THOMSON-CSF) 26 November 1986 (26.11.86)	1 - 3

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 1998 (15.09.98)	14 October 1998 (14.10.98)
Name and mailing address of the ISA/	Authorized officer
Facsimile No. RU	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

9xc1

Translation

09582206

2131

7

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference RU01-IF298	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/RU98/00182	International filing date (*day/month/year*) 19 June 1998 (19.06.98)	Priority date (*day/month/year*) 19 January 1998 (19.01.98)
International Patent Classification (IPC) or national classification and IPC H01L 9/00		
Applicant OTKRYTOE AKTSIONERNOE OBSCHESTVO "MOSKOVSKAYA GORODSKAYA TELEFONNAYA SET"		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
30 July 1999 (30.07.99)	04 April 2000 (04.04.2000)
Name and mailing address of the IPEA/RU Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/RU98/00182

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/RU 98/00182

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-3	YES
	Claims		NO
Inventive step (IS)	Claims	1-3	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-3	YES
	Claims		NO

2. Citations and explanations

Claims 1-3 fulfil the requirements of novelty and inventive step as none of the documents cited in the search report, either alone or in combination, discloses a method for the cryptographic conversion of binary data blocks in which the operation depending on the value of the j-th sub-block, where $j \leq N$, is a transposition operation of the bits in the i-th sub-block.

Т 9

ДОГОВОР О ПАТЕНТНОЙ КООПЕРАЦИИ

REC'D 24 MAY 2000

WIPO PCT

PCT

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

(статья 36 и правило 70 PCT)

№ дела заявителя или агента: RU01-IF/298	**Для дальнейших действий** см. уведомление о пересылке заключения международной предварительной экспертизы (форма PCT/IPEA/416).	
Номер международной заявки: PCT/RU 98/00182	Дата международной подачи: 19 июня 1998 (19.06.98)	Самая ранняя дата приоритета: 19 января 1998 (19.01.98)
Международная патентная классификация (МПК-7):	H04L 9/00	
Заявитель: МОЛДОВЯН Александр Андреевич и др.		

1. Данное заключение международной предварительной экспертизы подготовлено настоящим Органом международной предварительной экспертизы и направлено заявителю в соответствии со статьей 36 PCT.

2. Данное заключение содержит всего 3 листов, включая данный общий лист

☐ Данное заключение сопровождается также ПРИЛОЖЕНИЯМИ, т.е. листами описания, формулы и/или чертежей, которые были изменены и являются основой для данного заключения и/или листами, содержащими исправления, представленные настоящему Органу (см.Правило 70.16 и пункт 607 Административной инструкции PCT).

Упомянутые приложения содержат всего _____ листов

3. Данное заключение содержит информацию, относящуюся к следующим разделам

I ☒ Основа заключения

II ☐ Приоритет

III ☐ Отсутствие заключения относительно новизны, изобретательского уровня и промышленной применимости

IV ☐ Нарушение единства изобретения

V ☒ Утверждение относительно новизны, изобретательского уровня и промышленной применимости;ссылки и пояснения в обоснование утверждения (Статья 35(2))

VI ☐ Некоторые цитируемые документы

VII ☐ Некоторые дефекты международной заявки

VIII ☐ Некоторые замечания, касающиеся международной заявки

Дата представления требования: 30 июля 1999 (30.07.99)	Дата подготовки заключения: 04 апреля 2000 (04.04.2000)
Наименование и адрес Органа международной предварительной экспертизы: Федеральный институт промышленной собственности Россия, 121858, Москва, Бережковская наб., 30-1 Факс: 243-3337, телетайп: 114818 ПОДАЧА	Уполномоченное лицо: Д.Смирнов Телефон №: (095)240-2591

Форма PCT/IPEA/409 (общий лист) (июль 1998)

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

Международная заявка № PCT/RU 98/00182

I. Основа заключения

1. Элементы международной заявки:*

[x] международная заявка в том виде, в котором она была подана

[ ] описание:

страницы _____ первоначально поданные
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] формула изобретения:

страницы _____ первоначально поданные
страницы _____ поданные (вместе с объяснениями) по Статье 19
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] чертежи:

страницы _____ первоначально поданные,
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] часть описания, касающаяся перечня последовательностей:

страницы _____ первоначально поданные,
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

2. Все отмеченные выше элементы были поданы в настоящий Органу изначально или были представлены на языке, на котором была подана международная заявка, если иное не указано в данном пункте.
Эти элементы были поданы в настоящий Орган или были представлены на следующем языке _____ который является:

[ ] языком перевода, представленного для целей международного поиска (Правило 23.1 (в)).
[ ] языком публикации международной заявки (Правило 48.3 (в)).
[ ] языком перевода, представленного для целей международной предварительной экспертизы (Правило 55.2 и/или 55.3).

3. Относительно любой **последовательности нуклеотидов и/или аминокислот**, содержащейся в международной заявке, международная предварительная экспертиза была прповедена на основе перечня последовательностей:

[ ] содержащегося в международной заявке в письменной форме.
[ ] поданного вместе с международной заявкой в машиночитаемой форме.
[ ] представленного позже в настоящий Орган в письменной форме.
[ ] представленного позже в настоящий Орган в машиночитаемой форме.
[ ] Представлено утверждение о том, что позже представленный перечень последовательностей в письменной форме не выходит за пределы раскрытого в международной заявке в том виде, в каком она была подана.
[ ] Представлено утверждение о том, что информация, записанная в машиночитаемой форме, идентична перечню последовательностей в письменной форме.

4. [ ] Изменения привели к изъятию:
   [ ] страниц описания _____
   [ ] пунктов формулы №№ _____
   [ ] страницы/фиг. чертежей _____

5. [ ] Настоящее заключение составлено без учета (некоторых) изменений, так как они выходят за рамки первоначально поданных материалов заявки, как указано на дополнительном листе (Правило 70.2(c))**

* *Заменяющие листы, которые были представлены в Получающее ведомство в ответ на его предложение в соответствии со Статьей 14, расцениваются в данном заключении как "первоначально поданные" и не прикладываются к заключению, поскольку они не содержат исправлений (Правило 70.16 и 70.17)*

** *Любой заменяющий лист, содержащий такие изменения, должен быть рассмотрен в соответствии с пунктом 1 и приложен к данному заключению.*

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

Международная заявка № PCT/RU 98/00182

V. Утверждение в соответствии со ст.35(2) в отношении новизны, изобретательского уровня и промышленной применимости; ссылки и пояснения, подкрепляющие такое утверждение

1. Утверждение

Новизна (N)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ
Изобретательский уровень (IS)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ
Промышленная применимость (IA)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ

2. Ссылки и пояснения (правило 70.7)

Пункты 1-3 формулы изобретения удовлетворяют критериям новизна и изобретательский уровень, поскольку документы, цитируемые в отчете о поиске ни каждый в отдельности, ни в совокупности не раскрывают способа криптографического преобразования блоков двоичных данных в котором в качестве операции, зависящей от значения j-го подблока, где $j \leqslant N$, используется операция перестановки битов i-го подблока.

PCT

ЗАЯВЛЕНИЕ

Нижеподписавшийся просит рассматривать настоящую международную заявку в соответствии с Договором о патентной кооперации.

Заполняется получающим ведомством

Международная заявка №:

Дата международной подачи

Название получающего ведомства и штамп „Международная заявка PCT"

№ дела заявителя или агента *(по желанию) (не более 12 знаков)* 155A

Графа I НАЗВАНИЕ ИЗОБРЕТЕНИЯ

Способ криптографического преобразования блоков двоичных данных

Графа II ЗАЯВИТЕЛЬ

Имя и адрес: *(Фамилия указывается перед именем; для юридического лица - полное уставное наименование. Адрес должен включать название страны и почтовый индекс.)*

МОЛДОВЯН Александр Андреевич
MOLDOVYAN Alexandr Andreevich
Российская Федерация, 188710, г.Всеволожск,
Russian Federation, 188710, g.Vsevolozhsk,
ул.Александровская, д.88/2, кв.62
ul.Alexandrovskaya, d.88/2, kv.62

☒ Данное лицо является также изобретателем

Телефон №

Телефакс №

Телекс №

Государство *(т.е. страна)* гражданства: RU

Государство *(т.е. страна)* местожительства: RU

Данное лицо является заявителем для: ☒ всех указанных государств ☐ всех указанных государств, кроме США ☐ только США ☐ государств, указанных в дополнительной графе

Графа III ДРУГИЕ ЗАЯВИТЕЛИ И/ИЛИ (ДРУГИЕ) ИЗОБРЕТАТЕЛИ

Имя и адрес: *(Фамилия указывается перед именем; для юридического лица - полное уставное наименование. Адрес должен включать название страны и почтовый индекс.)*

МОЛДОВЯН Николай Андреевич
MOLDOVYAN Nikolay Andreevich
Российская Федерация, 188710, г.Всеволожск,
Russian Federation, 188710, g.Vsevolozhsk,
ул.Александровская, д.88/2, кв.58
ul.Alexandrovskaya, d.88/2, kv.58

Данное лицо является:

☐ только заявителем

☒ заявителем и изобретателем

☐ только изобретателем *(если помечено здесь, то не требуется заполнять ниже)*

Государство *(т.е. страна)* гражданства: RU

Государство *(т.е. страна)* местожительства: RU

Данное лицо является заявителем для: ☒ всех указанных государств ☐ всех указанных государств, кроме США ☐ только США ☐ государств, указанных в дополнительной графе

☐ Другие заявители и/или (другие) изобретатели названы на листе для продолжения.

Графа IV АГЕНТ ИЛИ ОБЩИЙ ПРЕДСТАВИТЕЛЬ; ИЛИ АДРЕС ДЛЯ ПЕРЕПИСКИ

Лицо, указанное ниже, настоящим назначается (назначено) представлять заявителя (заявителей) в компетентных международных органах в качестве: ☒ агента ☐ общего представителя

Имя и адрес: *(Фамилия указывается перед именем; для юридического лица - полное уставное наименование. Адрес должен включать название страны и почтовый индекс.)*

АНДРЕЕВ Владимир Иванович
ANDREEV Vladimir Ivanovich
Российская Федерация, 193036, Санкт-Петербург,
Russian Federation, 193036, St.Petersburg,
а/я 24 "Невинпат"
P.O.Box 24 "Nevinpat"

Телефон № (812)312-36-90

Телефакс № (812)312-21-65

Телекс №

☐ Пометить эту клетку, если агент или общий представитель не назначаются, а вместо этого выше указывается специальный адрес для переписки.

Графа V УКАЗАНИЕ ГО[redacted]АРСТВ

Настоящим делаются следующие указания в соответствии с правилом 4.9(a) *(сделать пометки в нужных клетках; должна быть помечена хотя бы одна клетка)*:

Региональный патент

- ☐ AP Патент ARIPO: KE Кения (Kenya), LS Лесото (Lesotho), MW Малави (Malawi), SD Судан (Sudan), SZ Свазиленд (Swaziland), UG Уганда (Uganda), а также любое другое государство, являющееся Договаривающимся государством Протокола Хараре и PCT
- ☐ EA Евразийский патент: AZ Азербайджан (Azerbaijan), BY Беларусь (Belarus), KZ Казахстан (Kazakstan), RU Российская Федерация (Russian Federation), TJ Таджикистан (Tajikistan), TM Туркменистан (Turkmenistan), а также любое другое государство, являющееся Договаривающимся государством Евразийской патентной конвенции и PCT
- ☒ EP Европейский патент: AT Австрия (Austria), BE Бельгия (Belgium), CH & LI Швейцария и Лихтенштейн (Switzerland and Liechtenstein), DE Германия (Germany), DK Дания (Denmark), ES Испания (Spain), FR Франция (France), GB Великобритания (United Kingdom), GR Греция (Greece), IE Ирландия (Ireland), IT Италия (Italy), LU Люксембург (Luxembourg), MC Монако (Monaco), NL Нидерланды (Netherlands), PT Португалия (Portugal), SE Швеция (Sweden), а также любое другое государство, являющееся Договаривающимся государством Европейской патентной конвенции и PCT
- ☐ OA Патент OAPI: BF Буркина-Фасо (Burkina Faso), BJ Бенин (Benin), CF Центральноафриканская Республика (Central African Republic), CG Конго (Congo), CI Кот-д'Ивуар (Côte d'Ivoire), CM Камерун (Cameroon), GA Габон (Gabon), GN Гвинея (Guinea), ML Мали (Mali), MR Мавритания (Mauritania), NE Нигер (Niger), SN Сенегал (Senegal), TD Чад (Chad), TG Того (Togo), а также любое другое государство, являющееся членом OAPI и Договаривающимся государством PCT *(если испрашивается иной охранный документ или статус, написать на пунктирной линии)* .....

Национальный патент *(если испрашивается иной охранный документ или статус, написать на пунктирной линии)*:

- ☐ AL Албания (Albania)
- ☐ AM Армения (Armenia) .....
- ☐ AT Австрия (Austria) .....
- ☐ AU Австралия (Australia) .....
- ☐ AZ Азербайджан (Azerbaijan)
- ☐ BB Барбадос (Barbados)
- ☐ BG Болгария (Bulgaria) .....
- ☐ BR Бразилия (Brazil) .....
- ☐ BY Беларусь (Belarus)
- ☐ CA Канада (Canada)
- ☐ CH & LI Швейцария и Лихтенштейн (Switzerland and Liechtenstein)
- ☒ CN Китай (China) .....
- ☒ CZ Чешская Республика (Czech Republic) .....
- ☐ DE Германия (Germany) .....
- ☐ DK Дания (Denmark) .....
- ☐ EE Эстония (Estonia) .....
- ☐ ES Испания (Spain) .....
- ☐ FI Финляндия (Finland) .....
- ☐ GB Великобритания (United Kingdom)
- ☐ GE Грузия (Georgia) .....
- ☐ HU Венгрия (Hungary) .....
- ☐ IS Исландия (Iceland)
- ☒ JP Япония (Japan) .....
- ☐ KE Кения (Kenya) .....
- ☐ KG Киргизстан (Kyrgyzstan) .....
- ☐ KP Корейская Народно-Демократическая Республика (Democratic People's Republic of Korea) .....
- ☒ KR Республика Корея (Republic of Korea) .....
- ☐ KZ Казахстан (Kazakstan) .....
- ☐ LK Шри Ланка (Sri Lanka)
- ☐ LR Либерия (Liberia)
- ☐ LS Лесото (Lesotho) .....
- ☐ LT Литва (Lithuania)
- ☐ LU Люксембург (Luxembourg) .....
- ☐ LV Латвия (Latvia)
- ☐ MD Республика Молдова (Republic of Moldova) .....
- ☐ MG Мадагаскар (Madagascar) .....
- ☐ MK Бывшая югославская Республика Македония (The former Yugoslav Republic of Macedonia) .....
- ☐ MN Монголия (Mongolia)
- ☐ MW Малави (Malawi) .....
- ☐ MX Мексика (Mexico) .....
- ☐ NO Норвегия (Norway)
- ☐ NZ Новая Зеландия (New Zealand) .....
- ☒ PL Польша (Poland) .....
- ☐ PT Португалия (Portugal) .....
- ☐ RO Румыния (Romania)
- ☐ RU Российская Федерация (Russian Federation) .....
- ☐ SD Судан (Sudan)
- ☐ SE Швеция (Sweden)
- ☐ SG Сингапур (Singapore)
- ☒ SI Словения (Slovenia) .....
- ☒ SK Словакия (Slovakia) .....
- ☐ TJ Таджикистан (Tajikistan) .....
- ☐ TM Туркменистан (Turkmenistan) .....
- ☐ TR Турция (Turkey) .....
- ☐ TT Тринидад и Тобаго (Trinidad and Tobago) .....
- ☒ UA Украина (Ukraine) .....
- ☐ UG Уганда (Uganda) .....
- ☒ US Соединенные Штаты Америки (United States of America) .....
- ☐ UZ Узбекистан (Uzbekistan) .....
- ☐ VN Вьетнам (Viet Nam) .....

Клетки, зарезервированные для указания государств (в целях получения национальных патентов), которые стали участниками PCT после выпуска данного листа:

- ☐ .....
- ☐ .....

В дополнение к указаниям, сделанным выше, заявитель, в соответствии с правилом 4.9(b), делает также все указания, допустимые в соответствии с PCT, за исключением указания (указаний) .....

Заявитель настоящим заявляет, что эти дополнительные указания подлежат подтверждению и что любое указание, не подтвержденное до истечения 15 месяцев с даты приоритета, должно считаться изъятым заявителем на момент истечения этого срока. *(Подтверждение указания состоит в подаче уведомления, содержащего указание, и в оплате пошлин за указание и за подтверждение. Подтверждение должно быть получено получающим ведомством в пределах 15-месячного срока.)*

Графа VI ПРИТЯЗАНИЕ НА ПРИОРИТЕТ

Последующие притязания на приоритет приведены в дополнительной графе ☐

Настоящим испрашивается приоритет следующей(их) предшествующей(их) заявки(ок):

Страна (в которую или в отношении которой была подана заявка)	Дата подачи (день/месяц/год)	Номер заявки	Ведомство подачи (только для региональных и международных заявок)
(1) RU	19 января 1998 (19.01.98)	98100685	
(2)			
(3)			

Пометить следующую клетку, если заверенная копия предшествующей заявки выдается ведомством, которое для настоящей международной заявки является Получающим ведомством (при условии уплаты установленной пошлины):

☒ Прошу Получающее ведомство направить Международному бюро заверенные копии заявок, указанных выше под № 98100685

Графа VII МЕЖДУНАРОДНЫЙ ПОИСКОВЫЙ ОРГАН

Выбор Международного поискового органа (ISA)
(Если компетентными в проведении международного поиска являются два или более международных поисковых органа, назвать один из них; можно использовать двухбуквенный код): ISA/_____

Предшествующий поиск *Заполняется, если у Международного поискового органа уже запрашивался поиск (международный, международного типа или иной) и его просят по возможности основывать международный поиск на результатах ранее проведенного поиска. Просьба идентифицировать поиск либо ссылкой на соответствующую заявку (или ее перевод), либо ссылкой на заказ на поиск:*

Страна *(или региональное ведомство):* Дата *(день/месяц/год):* Номер:

Графа VIII КОНТРОЛЬНЫЙ ПЕРЕЧЕНЬ

Настоящая международная заявка содержит следующее количество листов:

1. заявление	:	3 листов
2. описание	:	13 листов
3. формула	:	1 листов
4. реферат	:	1 листов
5. чертежи	:	4 листов
Всего	:	22 листов

К настоящей международной заявке приложены следующие документы:

1. ☐ отдельная подписанная доверенность
2. ☐ копия общей доверенности
3. ☐ разъяснения по поводу отсутствия подписи
4. ☐ приоритетный(е) документ(ы) *(указанные в графе VI под №):*
5. ☐ лист расчета пошлин
6. ☐ информация о депонировании микроорганизмов
7. ☐ перечень последовательностей нуклеотидов/аминокислот
8. ☐ прочее *(указать):*

Фигура № 1 чертежей (если имеются) предлагается для публикации с рефератом.

Графа IX ПОДПИСЬ ЗАЯВИТЕЛЯ ИЛИ АГЕНТА

Рядом с подписью назвать фамилию каждого подписавшего и указать, в каком качестве он подписал заявление, если это не очевидно из данных, приведенных в заявлении.

А.А.Молдовян

Н.А.Молдовян

Заполняется получающим ведомством

1. Дата фактического получения предполагаемой международной заявки:

2. Чертежи: ☐ получены ☐ не получены

3. Исправленная дата при более позднем, но своевременном получении страниц или чертежей, дукомплектовывающих предполагаемую международную заявку:

4. Дата своевременного получения требуемых исправлений согласно статье 11(2) PCT:

5. Международный поисковый орган, выбранный заявителем: ISA/

6. ☐ Направление копии для поиска задержано до уплаты пошлины за поиск.

Заполняется Международным бюро

Дата получения регистрационного экземпляра Международным бюро:

PCT

ГЛАВА II

ТРЕБОВАНИЕ

Требование согласно статье 31 Договора о патентной кооперации:
Нижеподписавшийся просит, чтобы международная заявка, указанная ниже стала предметом международной предварительной экспертизы согласно Договору о патентной кооперации

заполняется Органом международной предварительной экспертизы

Идентификация ОМПЭ	Дата получения требования

Графа I. ИДЕНТИФИКАЦИЯ МЕЖДУНАРОДНОЙ ЗАЯВКИ		№ дела заявителя (агента) RU01-IF/298
Номер международной заявки: PCT/RU98/00182	Дата международной подачи день/месяц/год) 19 июня 1998 (19.06.98)	Самая ранняя дата приоритета день/месяц/год) 19 января 1998 (19.01.98)

Название изобретения: **СПОСОБ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ БЛОКОВ ДВОИЧНЫХ ДАННЫХ**

Графа II. **ЗАЯВИТЕЛЬ**

Имя и адрес: *(фамилия указывается перед именем; для юридического лица полное уставное наименование. Адрес должен включать название страны и почтовый индекс)*	Телефон №
МОЛДОВЯН Александр Андреевич MOLDOVYAN Alexandr Andreevich RU, 188710, г. Всеволожск, ул. Александровская, д. 88/2, кв. 62 RU, 188710, g. Vsevolozhsk, ul. Alexandrovskaya, d. 88/2, kv. 62	Телефон № Телефон №

Государство *(т.е. страна)* гражданства: RU	Государство *(т.е. страна)* местожительства: RU

Имя и адрес: *(фамилия указывается перед именем; для юридического лица полное уставное наименование. Адрес должен включать название страны и почтовый индекс)*
МОЛДОВЯН Николай Андреевич MOLDOVYAN Nikolay Andreevich RU, 188710, г. Всеволожск, ул. Александровская, д. 88/2, кв. 58 RU, 188710, g. Vsevolozhsk, ul. Alexandrovskaya, d. 88/2, kv. 58

Государство *(т.е. страна)* гражданства: RU	Государство *(т.е. страна)* местожительства: RU

Имя и адрес: *(фамилия указывается перед именем; для юридического лица полное уставное наименование. Адрес должен включать название страны и почтовый индекс)*
Открытое акционерное общество "Московская Городская Телефонная Сеть" Otkrytoye aktsionernoye obschestvo "Moskovskaya Gorodskaya Telefonnaya Set" RU, 103804, Москва, ГСП, Дегтярный переулок, дом 6, строение 2. RU, 103804, Moskva, GSP, Degtyarnyi pereulok, dom 6, stroyeniye 2.

Государство *(т.е. страна)* гражданства: RU	Государство *(т.е. страна)* местожительства: RU

☐ Другие заявители указаны на листе для продолжения

Международная заявка № PCT/RU98/00182

Графа III. АГЕНТ ИЛИ ОБЩИЙ ПРЕДСТАВИТЕЛЬ: АДРЕС ДЛЯ ПЕРЕПИСКИ

Лицо, указанное ниже, является ☒ агентом, ☐ общим представителем

и: ☒ назначено ранее и представляет заявителя также и при проведении международной предварительной экспертизы

☐ настоящим назначается и любое предшествующее назначение агента/общего представителя отменяется

☐ настоящим назначается в дополнение к агенту(ам), назначенным ранее, специально для ведения дела в Органе международной предварительной экспертизы

Лицо, указанное ниже, настоящим назначается (назначено) представлять заявителя (заявителей) в компетентных международных органах в качестве: ☒ агента ☐ общего представителя

Имя и адрес: *(Фамилия указывается перед именем; для юридического лица — полное уставное наименование. Адрес должен включать почтовый индекс и название страны).*

ООО Центр ИННОТЭК
ООО Tsentr INNOTEC

RU, 105023, Москва, Б.Семеновская, д. 49, к. 404
RU, 105023, Moskva, B. Semenovskaya, d. 49, k. 404

Телефон № (095) 737-6377
(095) 366-9066

Телефакс № (095) 737-6366
(095) 366-9066

Телекс №

☐ Отметьте здесь, если агент или общий представитель не назначается, а выше специально указан адрес для переписки

Графа IV. ЗАЯВЛЕНИЕ, КАСАЮЩЕЕСЯ ИЗМЕНЕНИЙ

Заявитель желает, чтобы Орган международной предварительной экспертизы: *

(i) ☒ начал международную предварительную экспертизу на основе международной заявки, как была подана

(ii) ☐ принял во внимание изменения согласно статье 34, внесенные:

☐ в описание (изменения прилагаются)

☐ в формулу (изменения прилагаются)

☐ в чертежи (изменения прилагаются)

(iii) ☐ принял во внимание изменения формулы согласно статье 19, поданные в международное бюро (копия прилагается)

(iV) ☐ не принимал во внимание изменения формулы согласно статье 19 и считал их отозванными

(V) ☐ отложил начало международной предварительной экспертизы до истечения 20 месяцев с даты приоритета, если Орган не получит копию изменений согласно статье 19 либо извещение заявителя, что он не желает их делать (правило 69.1(d). (Данный квадрат может быть отмечен только если еще не истек срок согласно статье 19).

* Если не отмечено ни одного квадрата, международная предварительная экспертиза будет начата на основе международной заявки, как она была подана, или, если Орган международной предварительной экспертизы получит копию изменений формулы согласно статье 19 и/или изменения международной заявки согласно статье 34 до того, как он начнет подготовку письменного мнения, или заключения международной предварительной экспертизы, то с учетом этих изменений.

Графа V. ВЫБОР ГОСУДАРСТВ

☒ Заявитель настоящим делает выбор всех государств, выбор которых возможен *(т.е. всех указанных государств, связанных Главой II PCT)*.....
.....
.....
.....

(Если заявитель не желает выбрать некоторые государства, то наименование и двубуквенный код этих государств указывается выше)

Международная заявка № PCT/RU98/00182

Графа VI. КОНТРОЛЬНЫЙ ПЕРЕЧЕНЬ

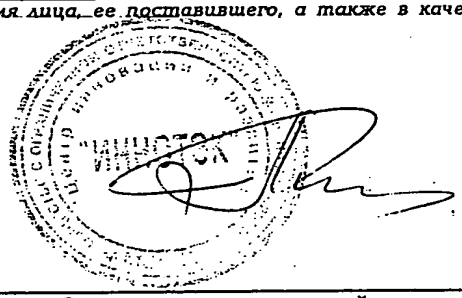
К требованию прилагаются следующие материалы для международной предварительной экспертизы:		Заполняется только Органом международной предварительной экспертизы: получено	не получено
1. Изменения по статье 34			
описание	листов	☐	☐
формула	листов	☐	☐
чертежи	листов	☐	☐
2. Сопроводительное письмо к изменениям по статье 34	листов	☐	☐
3. Копия изменений по статье 19	листов	☐	☐
4. Копия объяснений по статье 19	листов	☐	☐
5. Прочее (указать)	листов	☐	☐

К требованию прилагаются также следующие документы:

1. ☐ отдельная подписанная доверенность
2. ☐ копия общей доверенности
3. ☐ объяснение отсутствия подписи
4. ☒ лист расчета пошлины
5. ☐ прочее (*указать*)

Графа VII. ПОДПИСЬ ЗАЯВИТЕЛЯ, АГЕНТА ИЛИ ОБЩЕГО ПРЕДСТАВИТЕЛЯ

Рядом с каждой подписью укажите имя лица, ее поставившего, а также в качестве кого это лицо подписалось (если это не очевидно из чтения требования)



Руководитель
ООО Центр ИННОТЭК

Т.А. Вахнина

Заполняется Органом международной предварительной экспертизы

1. Дата фактического получения ТРЕБОВАНИЯ

2. Исправленная дата получения требования с исправлениями в соответствии с правилом 60.1 (b)

3. ☐ Требование получено по истечении 19 месяцев с даты приоритета ☐ Заявитель извещен об этом обстоятельстве

Заполняется Международным бюро

Требование получено из ОМПЭ:

ГЛАВА II

PCT
ЛИСТ РАСЧЕТА ПОШЛИН

Приложение к требованию на проведение международной предварительной экспертизы

заполняется Органом международной предварительной экспертизы

Международная заявка № PCT/RU98/00182	
№ дела заявителя (агента) RU01 – IF/298	
Заявитель: **МОЛДОВЯН Александр Андреевич и др.**	
РАСЧЕТ ПРЕДПИСАННЫХ ПОШЛИН (ТАРИФОВ)	
1. Тариф за предварительную экспертизу ..... 1260 руб.	
2. Пошлина за обработку ..... 162 USD	
(Если заявителя имеют право на уменьшение размера международной пошлины, то в ☐ указывается 25% от размера пошлины за обработку)	

Форма PCT/IPEA/40 (приложение) (январь 1996)

Пошлина (тариф) за международную предварительную экспертизу уплачивается за счет:

1. Для физических и юридических лиц из Москвы и Московской области: Получатель платежа – ИНН 7730036073
ВНИИГПЭ, р/с 150141702, банк получателя – Дорогомиловский филиал Элексбанка.
МФО 998372 (или 44583285), уч. 8Д

2. Для физических и юридических лиц из России и стран СНГ: Получатель платежа – ИНН 7730036073
ВНИИГПЭ, р/с 150141702 в Дорогомиловском филиале Элексбанка, корр/счет 5890603,
банк получателя – ГКРЦ ГУ ЦБ РФ
по г. Москве, корр/счет 285161000, МФО 201791 (или 44583001)

Пошлина за обработку уплачивается на счет 67087558/001 во Внешторгбанке РФ,
получатель платежа:
ИНН 7730036073 ВНИИГПЭ, адрес банка: 103031, Москва, Кузнецкий мост, 16.

Корреспонденция согласно Договору о патентной кооперации
от ОРГАНА МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

PCT

от 11 мая 2000 (11.05.2000)

УВЕДОМЛЕНИЕ О ПЕРЕДАЧЕ ЗАКЛЮЧЕНИЯ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ
(правило 71.1 Инструкции к PCT)

Кому: РФ, 105023, Москва,
Б.Семеновская
д.49, к.404
ООО Центр ИННОТЭК

№ дела заявителя: RU01-IF/298		**ВАЖНОЕ УВЕДОМЛЕНИЕ**
Номер международной заявки: PCT/RU 98/00182	Дата международной подачи: 19 июня 1998 (19.06.98)	Самая ранняя дата приоритета: 19 января 1998 (19.01.98)
Заявитель(имя): МОЛДОВЯН Александр Андреевич и др.		

1. Настоящим заявитель уведомляется, что Орган международной предварительной экспертизы направляет заключение международной предварительной экспертизы (с приложениями, если они имеются) по вышеуказанной международной заявке.

2. Копия заключения (с приложениями, если они имеются) направлены в Международное бюро для сообщения всем выбранным ведомствам.

3. В случае, если потребуется какому-либо выбранному ведомству, Международное бюро подготовит перевод на английский язык заключения (но без приложения) и направит такой перевод выбранным ведомствам.

4. **Внимание:**

Заявитель может начать национальную фазу раньше в каждом выбранном ведомстве осуществлением определенных действий (предоставлением переводов и уплатой национальных пошлин) в течение 30 месяцев с даты приоритета (или позднее в некоторых ведомствах) (Статья 39(1)) (смотри также напоминание, посланное Международным бюро с формой PCT/IB/301)

Когда перевод международной заявки должен быть представлен выбранному ведомству, то он должен содержать перевод любого приложения к заключению международной предварительной экспертизы. Последний делается под ответственность заявителя в каждое выбранное ведомство.

В отношении других приемлемых сроков и требований выбранных ведомств смотри Том II Руководства для заявителя PCT.

Наименование и адрес Органа международной предварительной экспертизы:	Уполномоченное лицо:
Федеральный институт промышленной собственности Россия, 121858, Москва, Бережковская наб., 30-1 Факс: 243-3337, телетайп: 114818 ПОДАЧА	Т.Владимирова Телефон №: (095)240-2591

Форма PCT/IPEA/416 (июль 1992)

ДОГОВОР О ПАТЕНТНОЙ КООПЕРАЦИИ

PCT

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

(статья 36 и правило 70 PCT)

№ дела заявителя или агента: RU01-IF/298	**Для дальнейших действий** см. уведомление о пересылке заключения международной предварительной экспертизы (форма PCT/IPEA/416).	
Номер международной заявки: PCT/RU 98/00182	Дата международной подачи: 19 июня 1998 (19.06.98)	Самая ранняя дата приоритета: 19 января 1998 (19.01.98)
Международная патентная классификация (МПК-7):	H04L 9/00	
Заявитель: МОЛДОВЯН Александр Андреевич и др.		

1. Данное заключение международной предварительной экспертизы подготовлено настоящим Органом международной предварительной экспертизы и направлено заявителю в соответствии со статьей 36 PCT.

2. Данное заключение содержит всего 3 листов, включая данный общий лист

☐ Данное заключение сопровождается также ПРИЛОЖЕНИЯМИ, т.е. листами описания, формулы и/или чертежей, которые были изменены и являются основой для данного заключения и/или листами, содержащими исправления, представленные настоящему Органу (см.Правило 70.16 и пункт 607 Административной инструкции PCT).

Упомянутые приложения содержат всего _____ листов

3. Данное заключение содержит информацию, относящуюся к следующим разделам

- I ☒ Основа заключения
- II ☐ Приоритет
- III ☐ Отсутствие заключения относительно новизны, изобретательского уровня и промышленной применимости
- IV ☐ Нарушение единства изобретения
- V ☒ Утверждение относительно новизны, изобретательского уровня и промышленной применимости;ссылки и пояснения в обоснование утверждения (Статья 35(2))
- VI ☐ Некоторые цитируемые документы
- VII ☐ Некоторые дефекты международной заявки
- VIII ☐ Некоторые замечания, касающиеся международной заявки

Дата представления требования: 30 июля 1999 (30.07.99)	Дата подготовки заключения: 04 апреля 2000 (04.04.2000)
Наименование и адрес Органа международной предварительной экспертизы: Федеральный институт промышленной собственности Россия, 121858, Москва, Бережковская наб., 30-1 Факс: 243-3337, телетайп: 114818 ПОДАЧА	Уполномоченное лицо: Д.Смирнов Телефон №: (095)240-2591

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

Международная заявка № PCT/RU 98/00182

I. Основа заключения

1. Элементы международной заявки:*

[X] международная заявка в том виде, в котором она была подана

[ ] описание:

страницы _____ первоначально поданные
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] формула изобретения:

страницы _____ первоначально поданные
страницы _____ поданные (вместе с объяснениями) по Статье 19
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] чертежи:

страницы _____ первоначально поданные,
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

[ ] часть описания, касающаяся перечня последовательностей:

страницы _____ первоначально поданные,
страницы _____ поданные вместе с требованием,
страницы _____ поданные с письмом от _____

2. Все отмеченные выше элементы были поданы в настоящий Органу изначально или были представлены на языке, на котором была подана международная заявка, если иное не указано в данном пункте.
Эти элементы были поданы в настоящий Орган или были представлены на следующем языке _____ который является:

[ ] языком перевода, представленного для целей международного поиска (Правило 23.1 (в)).
[ ] языком публикации международной заявки (Правило 48.3 (в)).
[ ] языком перевода, представленного для целей международной предварительной экспертизы (Правило 55.2 и/или 55.3).

3. Относительно любой последовательности нуклеотидов и/или аминокислот, содержащейся в международной заявке, международная предварительная экспертиза была проведена на основе перечня последовательностей:

[ ] содержащегося в международной заявке в письменной форме.
[ ] поданного вместе с международной заявкой в машиночитаемой форме.
[ ] представленного позже в настоящий Орган в письменной форме.
[ ] представленного позже в настоящий Орган в машиночитаемой форме.
[ ] Представлено утверждение о том, что позже представленный перечень последовательностей в письменной форме не выходит за пределы раскрытого в международной заявке в том виде, в каком она была подана.
[ ] Представлено утверждение о том, что информация, записанная в машиночитаемой форме, идентична перечню последовательностей в письменной форме.

4. [ ] Изменения привели к изъятию:
[ ] страниц описания _____
[ ] пунктов формулы №№ _____
[ ] страницы/фиг. чертежей _____

5. [ ] Настоящее заключение составлено без учета (некоторых) изменений, так как они выходят за рамки первоначально поданных материалов заявки, как указано на дополнительном листе (Правило 70.2(c))**

* *Заменяющие листы, которые были представлены в Получающее ведомство в ответ на его предложение в соответствии со Статьей 14, расцениваются в данном заключении как "первоначально поданные" и не прикладываются к заключению, поскольку они не содержат исправлений (Правило 70.16 и 70.17)*

** *Любой заменяющий лист, содержащий такие изменения, должен быть рассмотрен в соответствии с пунктом 1 и приложен к данному заключению.*

ЗАКЛЮЧЕНИЕ МЕЖДУНАРОДНОЙ ПРЕДВАРИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

Международная заявка № PCT/RU 98/00182

V. Утверждение в соответствии со ст.35(2) в отношении новизны, изобретательского уровня и промышленной применимости; ссылки и пояснения, подкрепляющие такое утверждение

1. Утверждение

Новизна (N)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ
Изобретательский уровень (IS)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ
Промышленная применимость (IA)	Пункты формулы	1-3	ДА
	Пункты формулы		НЕТ

2. Ссылки и пояснения (правило 70.7)

Пункты 1-3 формулы изобретения удовлетворяют критериям новизна и изобретательский уровень, поскольку документы, цитируемые в отчете о поиске ни каждый в отдельности, ни в совокупности не раскрывают способа криптографического преобразования блоков двоичных данных в котором в качестве операции, зависящей от значения j-го подблока, где $j \leqslant N$, используется операция перестановки битов i-го подблока.